Xournals

Academic Journal of Forensic Sciences

ISSN: 2581-4273 | Volume 05 | Issue 01 | April-2022

A Review on Criminal Profiling of Cyber Criminals

Niharika Pagare[1]

Available online at: www.xournals.com

Received 4th September 2021 | Revised 11th December 2021 | Accepted 23rd February 2022

Abstract:

A shift in paradigm of crime and criminals has been observed in the late half of the 20th century. With technology advancement, there has been advancement in crime and criminals too. NCRB data revealed that Computer Related crime formed the highest number of Cyber Crimes accounting for 75.2% during 2019. Cybercrime is an ever increasing threat to the security of computer systems. Profiling involves the analysis of personal characteristics or behavioural patterns, which allows an investigator to make generalizations about a person or a crime scene. Profiling employs analysis to determine whether a particular person may be engaged in a particular crime, as determined by evidence. Unlike traditional crime scenes that are tangible and have observable evidence, cybercrimes are not as easily examined and observed, there are no physical weapons or visible signs that might contribute to the art of profiling. Literature suggests the investigative tool of profiling had not been introduced in a courtroom until 1998. Criminal profiling gained popularity in serial offender cases, specifically serial killer cases. Criminal profiling, however, has increased its use in cybercrimes throughout the years since the development of computers and the Internet. Throughout the history of both criminal profiling and cybercrime, there have been many uses for criminal profiling but one primary objective has been identifying and understanding the criminal. This review paper aims to study the integration of two fields that is Forensic Psychology and Cyber forensics. Criminal profiling of Cyber Criminals in current era can help in monitoring and preventing Cybercrimes. By understanding online offenders and their pathways towards deviant behaviours, we can better identify steps that need to be taken to prevent such criminal activities.

Keywords: *Criminal Profiling, Cyber Crime, Cyber Criminals, Personality Traits, Cyber Trials, Cyber Behaviour.*

Authors:

1. *Institute of Forensic Science, Mantralaya, Fort, Mumbai, Maharashtra, INDIA.*

Introduction

With the increase in the number of crimes in cyberspace, the detection, investigation and apprehension of cybercriminals have also been comparatively difficult. With changing methods and interdisciplinary approaches, there can be assistance to the criminal justice system.

Profiling is a systemic linking of physical, behavioural, or psychological characteristics to specific offences and their use as a basis for making law enforcement decisions. The goal of profiling is to aid the criminal justice system in battling against crime, to provide a social and psychological assessment of the offender; a psychological evaluation of belongings found in the possession of the offender.

Criminal Profiling, an investigative approach, is based on the assumption that the crime scene provides details about the offence and the offender. The term "offender profiling" was introduced in the 1970s, linked to the activities of the FIB analysis unit. Initially, criminal profiling was used for serial murders, but the boundaries of research expanded and are now linked to various criminal offences such as rape, torture, murder, terrorism, cybercrime, etc. Historically the prominent uses of criminal profiling involved famous cases such as Jack the Ripper and Adolf Hitler. In the criminal profiling timeline, the investigative tool - Profiling had not been introduced in a courtroom until 1998 (FBI).

Cyber Crime is a broad term that covers any criminal activity that involves a computer or the Internet. People who commit cybercrime can be termed Cybercriminals. Website hijacking, phishing, credential attack, malware attack, DDoS, information theft, etc. are all broad types of cyber-attacks. The cost of a cyber-attack is huge. For example, the Denial of Service attack (DoS) attack in 2000 caused huge financial damage to companies such as Amazon, eBay, Dell, and CNN.

Virtual Crime Scene: The computer and the Internet can be seen as virtual crime scenes, respectively. Steps taken at a physical crime scene can also be associated with a virtual environment.

A Cyber trail is considered a virtual version of a signature left at a crime scene. Such evidence lead us to link the suspect to a computer crime/ virtual crime scene. The possibility of links between cybercrime investigations will also reduce the statistic of unsolved cyber cases. Investigators can connect each attack in the separate companies to one hacker/hacker group due to the cyber-trail they might leave behind. Cybercrime cases that involve multiple victims tend to leave a cyber-trail that can accidentally connect their work with another cybercrime investigation

Approaches to profile Cyber Criminals

In the history of both criminal profiling and cybercrime, there have been many uses for criminal profiling but one primary objective: identify and understand the criminal. Approaches to criminal profiling are:

Inductive Profiling

It rests with a simple premise, an assumption that similar crimes may also share some common personality traits. Information can be gathered from past crimes, past known offenders, and other sources of information, including the media. It helps investigators identify links to other cases. For example, a profiler can conclude that a criminal suffers from paranoia and is unemployed or works from home using statistics from previous cases to infer that the criminal may fall into the same type of pattern.

Deductive Profiling

By proper and thorough analysis of the crime scene and evidences left at that scene, the profiler can construct a mental picture of the unknown offender. It incorporates theories made at a crime scene, constructed hypotheses and observations based on the evidence. For example, forming a profile of a cyber-stalker. An analysis of the internet cache shows a user accessing a local online newspaper after he/she hacked a local business's network. This person of interest accessed the website up to 100 times a day. Now, it can be inferred that the criminal has tendencies to be paranoid. A criminal profiler may also infer that the criminal is also either unemployed or works from home and spent his time after the crime stalking the local news websites. An advantage of using a deductive profiling process is that it takes into account criminal behaviour as it evolves throughout the investigation.

Behavioural Evidence Analysis

Here stages include equivocal forensic analysis, victimology, assessment of crime scene, and criminal characteristics. It has been used by the FBI's Behavioural Analysis Unit to add significance to obtained computer forensic evidence as well as aid investigators with the reconstruction of the crime. BEA would be categorized as a deductive strategy.

4 stages (Figure No. 1) include equivocal forensic analysis, victimology, assessment of crime scene, and criminal characteristics **(Turvey, 2011).**

BEA can provide specific direction based on the behavioural characteristics of both the victim and the cybercriminal. Based on BEA, the profile of cyberstalkers can be made (Figure No. 2).

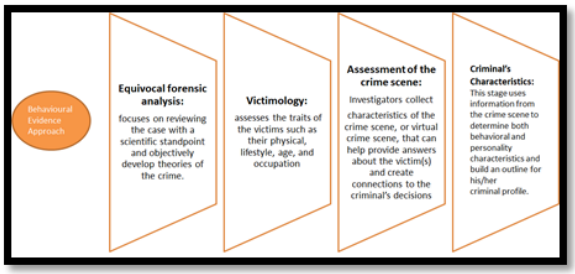

Figure No. 1: 4 Stages of equivocal Forensic Analysis, Victimology, Assessment of Crime Scene, and Criminal Characteristics

Figure No. 2: Cyber Stalker Profiling

Computer Forensics and Criminal Profiling Relationship

Computer forensics is applied during this step and includes system analysis that has been brought in for questioning by investigators as well as network analysis.

System analysis includes forensic analysis of the file systems found on a cybercriminal's or victim's computer. This type of analysis can help examiners detect any modified files and their content. The examination of log file entries is included as well. A computer forensic examiner approaches the computer like they would a crime scene and analyze any clues left behind by the cybercriminal. The examiners look for signatures (digital footprints), log files, Internet cache, images, file metadata, and social networking sites. Like physical evidences are considered as trails left behind by the perpetrator (on basis of Locard's Principle of exchange), digital evidence or trails may also be left behind by the cybercriminals- called digital/cyber trails or digital footprints.

Log files reveal the applications used. Keywords of web browsers can reveal websites visited and internet cache, which can help know the probable motive and modus operandi. The image file metadata and file metadata, especially in SEIC -Sexually Exploitative Imagery of Children, can reveal the interest in paraphilic themes like bestiality. Date created, last modified, last opened) indicates that the user showed interest in viewing the contents of the file(s). Metadata, such as timestamps of posts or blog entries, IP addresses, can be collected from Application Program Interfaces (APIs) such as Facebook, Twitter, etc. cybercriminal who wishes to commit a crime for financial gain, tend to do so with online fraud schemes using a Facebook profile and post a link to a fake fundraising page to collect money. Online sexual predators who use social media to attract children have been found to have a presence already online and understood how to navigate sites such as Twitter and communication apps like WhatsApp or Snapchat.

Personal habits are revealed or be detected in the cybercriminal's writing: nicknames, any pattern of typing mistakes, particular phrases, and writing style from uncovered text files. Some of these characteristics such as typing mistakes and writing style can be incorporated when a criminal profiler develops the potential education level in a cybercriminal profile. The number of grammatical errors and faulty sentence structure has shown to indicate levels of either high school dropout, high school graduate, college-educated, or upper-level education

Review of Literature

Raoul (2017) started the Hacker Profile Project (HPP) at United Nations, Consultant on Cybercrime Interregional Crime and Justice Research Institute (UNICRI) at Counter Human Trafficking and Emerging Crimes Unit. It aimed at analysing the hacking phenomenon in technological, social, economic aspects through criminological and technical approaches, to gain insight of various motivating factors involved, to implement profiling methodology to collect data as to who, where, when and why and to acquire and spread awareness and knowledge. The project phases consisted of the questionnaire with two typologies, full and compact and three modules A B and C. The Evaluation and Correlation Standards were Modus Operandi (MO), hacking career, motivations, lone or group hacker, selected targets, the principle of hacker's ethics,

crashed or damaged systems, perception of the illegality of their own activity and effect of laws, convictions and technical difficulties as a deterrent. The detailed analysis and correlation of profile were built on a scale of amateur to a professional that is wannabe lamer to military hacker and presented.

Nykodym *et al*. (2005) studied the origin of criminal profiling and its use infamous cases. Two profiling approaches were studied, one, Prospective profiling that creates a profile, using characteristics of previous crimes of specific offenders. Retrospective profiling which is used by the FBI is fact-specific and case-specific and links the specific person to a specific crime using evidence left behind by them. The Behavioural Evidence Analysis (BEA).

Turvey (2011) consists of 4 stages that are equivocal Forensic analysis, victimology, crime scene characteristics and offender characteristics. These stages can be applied to two phases: the Investigative phase and the Trial phase. The study presents statistics on cyber-attacks on business and factors that lead to such growing threats. Statistical data on insider crimes and abuse shows how the position of the attacker in the company has a significant influence on cybercrime. By applying BEA to insider threat/attackers, a profile of saboteur/spies can be initiated.

Lickiewicz (2011) proposed an Offender Psychological profile, a construct assuming the relation between psychological characterises and modus operandi of the offender which intend to serve as a creation of a psychological profile of a cybercrime perpetrator. Cyber criminality and methods of combating it were studied. A hacker profile model is proposed using the base aspects of the 5 Factor Theory. It attempts to indicate the relationship between the offender's characteristics, environment and their success and the modus operandi during the attack. It assumes the existence of dependence between the modus operandi of the perpetrator and central elements identified in him/her. The characteristics of the five factors are Intelligence, Personality, Social Skills, Technical Skills and Addiction to the Internet and are of equal importance for making the central elements. The Biological and External Environment influence the central elements. There is also the presence of the number of internal relations between central elements themselves. Central elements influence motivation to act, and this influences the selection of a victim. They in turn influence the method of attack; effectiveness of attack; methods used and mode of operation of the scene. Appropriate analysis of data from the crime scene allows inferring about central elements. The possibility of applying this model in such a way indicates that it has a practical dimension.

Long and Hadsell (2012) studies hackers intensively to offer a criminal profile or a Hacker Profile. Profiles could be made using techniques such as brainstorming, mind mapping, etc. The study suggests using Indications and warnings or I&W, a traditional military analytical method that studies past activity patterns to predict future events. By combining profiling and I&W, cyber-attacks may be averted. by examining the strategy, tactics, triggers, target, leadership, history, motivation, etc., a pool of information can be gained. A hacker checklist was created based on the factors mentioned and it was analysed to make a probable profile.

Saroha (2014) Identified key personality characteristics of cybercriminals end outlined a behavioural profile for cybercriminals. A sample of 20 participants was chosen from Delhi and NCR within an academic background of social sciences that is psychology and sociology. The age of the participants ranged from 18 to 25 years and it included both the genders. Sweet present it opens the participants were intensively interviewed through open-ended interview format questions. The study identified characteristics that were inherent in cybercriminals and which are understood as precursors of criminal behaviour the use academic knowledge as well as personal experience was used to come up with characteristics of cybercriminals the responses were identified and then classified under common headings and finally, a profile has constructed the characteristics stated by the respondents were classified under four major heads the technical knowhow personal traits social characteristics and motivation factors. Since this research included the opinion only of the students and not the professional there can be more research in the professional area for further studies.

Kapetanakis *et al*. (2014) studied the characteristics of a specific attacker behind a security incident. Technical security mechanisms have always focused on the attack's characteristics rather than the attacker. Finding the attacker's characteristics is a challenging problem, as relevant data cannot easily be found. They argue that the cyber traces left by a human attacker during an intrusion attempt can help towards building a profile of that particular person. To illustrate the same they developed an approach using case-based reasoning that indirectly measures an attacker's characteristics for given attack scenarios. It can be used to assist security and forensic investigators in profiling human attackers.

Grigaliunas and Toldinas (2016) proposed a method for digital evidence investigation using habits attribution. The main idea is to identify habits, attribute them and then create a profile of the attributed habits. Created profile as a set of habits and attributes may be used in digital evidence investigation to reduce the numbers of evidence sequences from a set of digital user places. A general framework for the analysis and the acquisition of digital evidence contained three basic domains: attribution, profiling and habits. The framework also outlines a context of the selected domains: for the attribution domain - metadata and other logs can be used to attribute actions to personality identification, for the profiling domain - profiles help reconstruct the crime, when there are too many unknowns, and for habits domain - approach to examining and classifying user habits.

Garcia (2018) studied the use of criminal profiling in cyber investigations. The primary objective of criminal profiling and its role in cybercrime investigation is to identify and understand the criminal. The profiling process involves two approaches. Firstly deductive profiling implies theory making at the crime scene, constructing hypotheses, evidences based on observation and conforming to the arrest being made. The second is the inductive approach which assists investigators to identify links to other or previous cases. It uses statistical analysis or comparison to group criminals committing a similar type of crimes to infer later. Several profiling frameworks have been analysed. One of them is the hacking profiling project which categorizes hackers from amateur to professional is from wanna be lamer to military hackers. But the drawback is that it only considers hackers and no other types of cybercriminals. The Behavioural Evidence Analysis (BEA) framework has 4 stages. The first stage, the equivocal Forensic analysis reviews case with a scientific viewpoint and develops theories objectively based on computer forensics techniques such as system and log analysis, hash value, etc. The second stage victimology focuses on traits of the victim's lifestyle, occupation, age, etc. The third stage is an assessment of the crime scene which is treated as a virtual crime scene wherein investigators assess and collect the cyber trials and digital evidence. Log files, keywords searching in web browsers, application logs, image and file metadata analysis specifically in (sexually exploitative imagery of children- SEIC). The fourth stage is criminal characterisation which makes use of information gathered from the crime scene to determine personality and behavioural characteristics for building criminal profiling of the cybercriminal. The criminal profile of hackers, internal and phishers was also framed.

Kipane (2019) studied the meaning of profiling cybercriminals in a security context. This study aims at describing the criminal aspects of cybercriminals for criminal profiling. Intensive research was made of previous researchers by the author in of. The study noted two approaches of criminal profiling, one is a prospective approach based on the data of characteristics of previously detained offenders and the second, retrospective approach, based on the study of personality and behaviour by analysis of the crime scene facts and circumstances of criminal offences. The criminogenic research identified individual peculiarities leading to the commission of a crime. The personality of a criminal is a complex system of needs, temperament and value orientation. Also, criminal personality formation, like individual personality formation, is determined by three factors such as heredity, socialization and self. The study identifies three traditional approaches of criminal profiling that is the criminal investigative approach that relies on tactics and evidence-based expert knowledge. Second is the clinical practitioner's approach wherein the clinical profilers draw up their conclusions only offenders trade from their clinical experience which is obtained by working with different offenders. The third is the statistical approach which includes statistical data and databases to find out the relationship between the information recorded in statistical reports and features of the offenders and using similar data cases and criminal offences detected previously. There is also mention of geographical profiling which uses the location of the offender's crime scene as the starting point to predict the area in which the offenders live. The profile of a cybercriminal is a combination of individual behaviour and qualities which are created without knowing their identity. Thus profiling involves the identification of unknown criminals using several techniques such as one, Analysing a crime scene, second determining the peculiarities of criminal offences and third, characterization of the personality of a criminal. The profile of cybercriminals described the following key factor:

a) Personality traits or characteristics,
b) criminal professionalism,
c) technical knowledge,
d) social characteristics which include democratic features and
e) characteristics of motivation etc.

The author also suggests the view that process of the profiling cybercriminals consists of four interrelated and successive stages which include

a) victimological aspect that can be described using routine activities theory (RAT) and general theory;
b) the motives of criminal which can include financial gain, emotional motive, the motive of self-affirmation or self-respect, sexual impulses or

c) desires, political-ideological or religious motives, just for a fun motive;
d) identification of features or properties by using inductive or deductive profiling;
e) digital behavioural analysis that uses digital forensics and technology and its application to digital footprints of criminal.

Kodippili (2020) studied the psychological and social aspects and their relationship with cybercrime. An attempt was made to identify the psychology of cybercriminals, especially of the hackers. Reasons for computer vulnerabilities were studied such as easy access, negligence, lack of storage space and mislaying of proof. Modes and ways of committing cyber-crime like data didling, email bombing, salami attack, DoS attack, virus attack, logic bombs, internet time theft and web jacking. The psychological aspects of hackers were studied. A profile of the hacker has been assessed. From studying the global cybercrime pattern, a framework was proposed. The profile of hackers can be extended to types of hackers and their choice of cybercrime based on their psychological description such as Grey Hat hackers who are self-motived and are hacktivists with their own motive. Black Hat hackers may be termed, narcissists. A model of hacker profile was made by surveying 546 people and the feedback was used to identify the environment they use for hacking. The personality, capabilities and deep perception have also been discussed. Thus a correlation has been made between psychological aspects and cybercrime.

Bada and Nurse (2021) made intensive review research based on the method that included protocol registration, criteria, sources of information, searching and selecting the article and collecting data. The study resulted in selecting 39 articles from 14 years (2006-2020) and adopting PRISMA for research review. The state-of-the-art in criminal profiling of cyber suggests the major use of hacker characterization and use of deductive approach of profiling.

Shree and Dhaliwal (2021) studied Behavioural Evidence Analysis (BEA) in detail for the existing literature, the approach and process models. They proposed a standardised approach for implementing the BEA technique to digital forensics (DF). Traditional digital forensic processes and BEA have been compared. Behavioural digital forensics models such as the 3 stage model, 4 stage model and 6 stage model have been described which show the implementation of BEA in digital forensic analysis. The authors proposed a model that integrates the two.

Discussion

The premise of any investigation is the evidences found on the crime scene. The crime scene, perpetrator and evidences are linked and each of the elements contributes and influence one another. Criminal profiling has been, in history, and assistive investigative tool to characterise a criminal based on the approaches such as deductive, inductive, behavioural evidences analysis, geographical profiling etc. the personality characteristics, motivating factors, technological assistance and interest, etc. can help in making the criminal profile. With the advent of technology, the methods of criminal activities have changed, yet, as Locard's Principle suggest - every contact leaves a trace- the digital footprints or cyber trials can be used as digital evidences to characterise cybercriminals by analysing cybercrimes. The literature reveals that criminal profiling of cybercriminals is yet in a nascent stage of research and has a lot of scopes. Digital behaviour analysis, digital profiling, idiographic studies, etc. are seen to have future prospects.

Conclusion

With an immense literature gap in both the field of criminal profiling and cybercrime investigations, a lot can be researched in multidisciplinary aspects. The review paper attempts to present a link between two distinct fields of forensic science. The research domain still being at a nascent stage, a lot of drawbacks are identified such as the presence of multiple types of cybercrimes, the argument can arise that one profile of a cybercriminal may not necessarily fit the profile of another. Hence the goal is to examine the types of cybercrime and develop profiles that help set a foundation for investigators.

References:

Bada, Maria, and Jason R. C. Nurse. "Profiling the Cybercriminal: A Systematic Review of Research." *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2021. *Crossref*, doi:10.1109/cybersa52016.2021.9478246.

Garcia, Natasha. "The use of criminal profiling in cybercrime investigations". Diss. Utica College, 2018.

Grigaliunas, Sarunas, and Jevgenijus Toldinas. "Digital Evidence Investigation Using Habits Attribution." *Proceedings of The 4th International Virtual Research Conference In Technical Disciplines*, 2016. *Crossref*, doi:10.18638/rcitd.2016.4.1.86.

Lickiewicz, Jakub "Cyber Crime Psychology – Proposal of an Offender Psychological Profile." Problems of Forensic Sciences, vol. 87, 2011, pp. 239–52, www.forensicscience.pl/pfs/87_Lickiewicz.pdf.

Kapetanakis, S. et al. "Profiling Cyber Attacks using Case-based Reasoning". *19th UK Workshop on Case-Based Reasoning.* N.p., 2014. 39–48.

Kipane, Aldona. "Meaning of Profiling of Cybercriminals in the Security Context." *SHS Web of Conferences*, edited by U. Berkis and L. Vilka, vol. 68, 2019, p. 01009. *Crossref*, doi:10.1051/shsconf/20196801009.

Kodippili K.A.S.G. *Profile of Cyber Criminal*. Faculty of Information Technology University of Moratuwa, 2020 https://www.researchgate.net/publication/346469807_Profile_of_Cyber_Criminal.

Long, Larisa April, and Egan Hadsell. "Profiling Hackers." *Global Information Assurance Certification Paper*, SANS Institute. 26 Jan. 2012, pp. 1–19., www.giac.org/paper/gsec/12321/profiling-hackers/115232.

Nykodym, Nick, et al. "Criminal Profiling and Insider Cyber Crime." *Digital Investigation*, vol. 2, no. 4, 2005, pp. 261–67. *Crossref*, doi:10.1016/j.diin.2005.11.004.

Raoul Chiesa "The Hackers Profiling Project (HPP)." Studylib.Net, *United Nations, Consultant on cybercrime, Interregional Crime and Justice Research Institute (UNICRI), Counter Human Trafficking and Emerging Crimes Unit,* 12 Feb. 2017, https://studylib.net/doc/18228394/the-hackers-profiling-project--hpp-

Saroha, Rashmi. "Profiling a Cyber Criminal." International Journal of Information and Computation Technology, vol. 4, no. 3, 2014, pp. 253–58. International Research Publications House, www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf.

Shree, Barkha, and Parneeta Dhaliwal. "Behavioural Evidence Analysis." *International Journal of Digital Crime and Forensics*, vol. 13, no. 5, 2021, pp. 20–42. *Crossref*, doi:10.4018/ijdcf.20210901.oa2.

Turvey, Brent. *Criminal Profiling: An Introduction to Behavioral Evidence Analysis*. 4th ed., Academic Press, 2011.